

00680599 " 100600

What Is Claimed Is:

1 1. A method for managing encryption within a database system that is
2 managed by a security administrator, wherein encryption is performed
3 automatically and transparently to a user of the database system, wherein users of
4 the database system are managed by a user administrator, the method comprising:
5 receiving a request to store data in a column of the database system,
6 wherein the column is designated as an encrypted column;
7 in response to receiving the request, automatically encrypting data using an
8 encryption function, wherein the encryption function uses a key stored in a keyfile
9 managed by the security administrator; and
10 storing data in the database system using a storage function of the database
11 system.

1 2. The method of claim 1, further comprising:
2 receiving a request to retrieve data from the encrypted column of the
3 database system;
4 if the request to retrieve data is received from the database administrator,
5 preventing the database administrator from decrypting encrypted data;
6 if the request to retrieve data is received from the security administrator,
7 preventing the security administrator from decrypting encrypted data; and
8 if the request to retrieve data is from an authorized user of the database
9 system, allowing the authorized user to decrypt encrypted data.

1 3. The method of claim 1, wherein the security administrator selects
2 one of, data encryption standard (DES) and triple DES as a mode of encryption
3 for the column.

09680599.100600

1 4. The method of claim 1, wherein the security administrator, the
2 database administrator, and the user administrator are distinct roles, and wherein a
3 person selected for one of these roles is not allowed to be selected for another of
4 these roles.

1 5. The method of claim 1, wherein managing the keyfile includes, but
2 is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;
5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;
7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and
10 moving an obfuscated copy of the keyfile to a volatile memory within a
11 server associated with the database system.

1 6. The method of claim 1, wherein upon receiving a request from the
2 security administrator specifying the column to be encrypted, if the column
3 currently contains data, the method further comprises:
4 decrypting the column using an old key if the column was previously
5 encrypted; and
6 encrypting the column using a new key.

00660599.100600

1 7. The method of claim 5, wherein the key identifier associated with
2 the encrypted column is stored as metadata associated with a table containing the
3 encrypted column within the database system.

1 8. The method of claim 5, further comprising establishing encryption
2 parameters for the encrypted column, wherein the encryption parameters include
3 encryption mode, key length, and integrity type by:
4 entering encryption parameters for the encrypted column manually; and
5 recovering encryption parameters for the encrypted column from a profile
6 table in the database system.

1 9. A computer-readable storage medium storing instructions that
2 when executed by a computer causes the computer to perform a method for
3 managing encryption within a database system that is managed by a security
4 administrator, wherein encryption is performed automatically and transparently to
5 a user of the database system, wherein users of the database system are managed
6 by a user administrator, the method comprising:
7 receiving a request to store data in a column of the database system,
8 wherein the column is designated as an encrypted column;
9 in response to receiving the request, automatically encrypting data using an
10 encryption function, wherein the encryption function uses a key stored in a keyfile
11 managed by the security administrator; and
12 storing data in the database system using a storage function of the database
13 system.

1 10. The computer-readable storage medium of claim 9, the method
2 further comprises:

00680599-100600

1 receiving a request to retrieve data from the encrypted column of the
2 database system;
3 if the request to retrieve data is received from the database administrator,
4 preventing the database administrator from decrypting encrypted data;
5 if the request to retrieve data is received from the security administrator,
6 preventing the security administrator from decrypting encrypted data; and
7 if the request to retrieve data is from an authorized user of the database
8 system, allowing the authorized user to decrypt encrypted data.

1 11. The computer-readable storage medium of claim 9, wherein the
2 security administrator selects one of, data encryption standard (DES) and triple
3 DES as a mode of encryption for the column.

1 12. The computer-readable storage medium of claim 9, wherein the
2 security administrator, the database administrator, and the user administrator are
3 distinct roles, and wherein a person selected for one of these roles is not allowed
4 to be selected for another of these roles.

1 13. The computer-readable storage medium of claim 9, wherein
2 managing the keyfile includes, but is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;
5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;
7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and

09680599.100600

10 moving an obfuscated copy of the keyfile to a volatile memory within a
11 server associated with the database system.

1 14. The computer-readable storage medium of claim 9, wherein upon
2 receiving a request from the security administrator specifying the column to be
3 encrypted, if the column currently contains data, the method further comprises:
4 decrypting the column using an old key if the column was previously
5 encrypted; and
6 encrypting the column using a new key.

1 15. The computer-readable storage medium of claim 13, wherein the
2 key identifier associated with the encrypted column is stored as metadata
3 associated with a table containing the encrypted column within the database
4 system.

1 16. The computer-readable storage medium of claim 13, wherein the
2 method further comprises establishing encryption parameters for the encrypted
3 column, wherein the encryption parameters include encryption mode, key length,
4 and integrity type by:
5 entering encryption parameters for the encrypted column manually; and
6 recovering encryption parameters for the encrypted column from a profile
7 table in the database system.

1 17. An apparatus that facilitates managing encryption within a
2 database system that is managed by a security administrator, wherein encryption is
3 performed automatically and transparently to a user of the database system,

00680599.100600

4 wherein users of the database system are managed by a user administrator,
5 comprising:
6 a receiving mechanism that is configured to receive a request to store data
7 in a column of the database system, wherein the column is designated as an
8 encrypted column;
9 an encrypting mechanism that is configured to encrypt data using an
10 encryption function, wherein the encryption function uses a key stored in a keyfile
11 managed by the security administrator; and
12 a storing mechanism that is configured to store data in the database system
13 using a storage function of the database system.

1 18. The apparatus of claim 17, further comprising:
2 the receiving mechanism that is further configured to receive a request to
3 retrieve data from the encrypted column of the database system;
4 an access mechanism that is configured to prevent the database
5 administrator and the security administrator from decrypting encrypted data; and
6 wherein the access mechanism is configured to allow an authorized user
7 of the database system to decrypt encrypted data.

1 19. The apparatus of claim 17, further comprising a selection
2 mechanism that is configured to select one of, data encryption standard (DES) and
3 triple DES as a mode of encryption for the column.

1 20. The apparatus of claim 17, wherein the security administrator, the
2 database administrator, and the user administrator are distinct roles, and wherein a
3 person selected for one of these roles is not allowed to be selected for another of
4 these roles.

00680599 " 4086000

1 21. The apparatus of claim 17, further comprising:
2 a creating mechanism that is configured to create the keyfile;
3 an establishing mechanism that is configured to establish a plurality of
4 keys to be stored in the keyfile;
5 wherein the establishing mechanism is further configured to establish a
6 relationship between a key identifier and the key stored in the keyfile;
7 a storing mechanism that is configured to store the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and
10 a moving mechanism that is configured to move an obfuscated copy of the
11 keyfile to a volatile memory within a server associated with the database system.

1 22. The apparatus of claim 17, further comprising:
2 a decrypting mechanism that is configured to decrypt the column using a
3 previous key if the column was previously encrypted; and
4 wherein the encrypting mechanism is further configured to encrypt the
5 column using a new key.

1 23. The apparatus of claim 21, wherein the key identifier associated
2 with the encrypted column is stored as metadata associated with a table containing
3 the encrypted column within the database system.

1 24. The apparatus of claim 21, wherein the establishing mechanism is
2 further configured to establish encryption parameters for the encrypted column,
3 wherein encryption parameters include encryption mode, key length, and integrity
4 type, and wherein the establishing mechanism includes:

- 5 an entering mechanism that is configured to enter encryption parameters
6 for the encrypted column manually; and
7 a recovering mechanism that is configured to recover encryption
8 parameters for the encrypted column from a profile table in the database system.

Add
a1

09680599-100600